

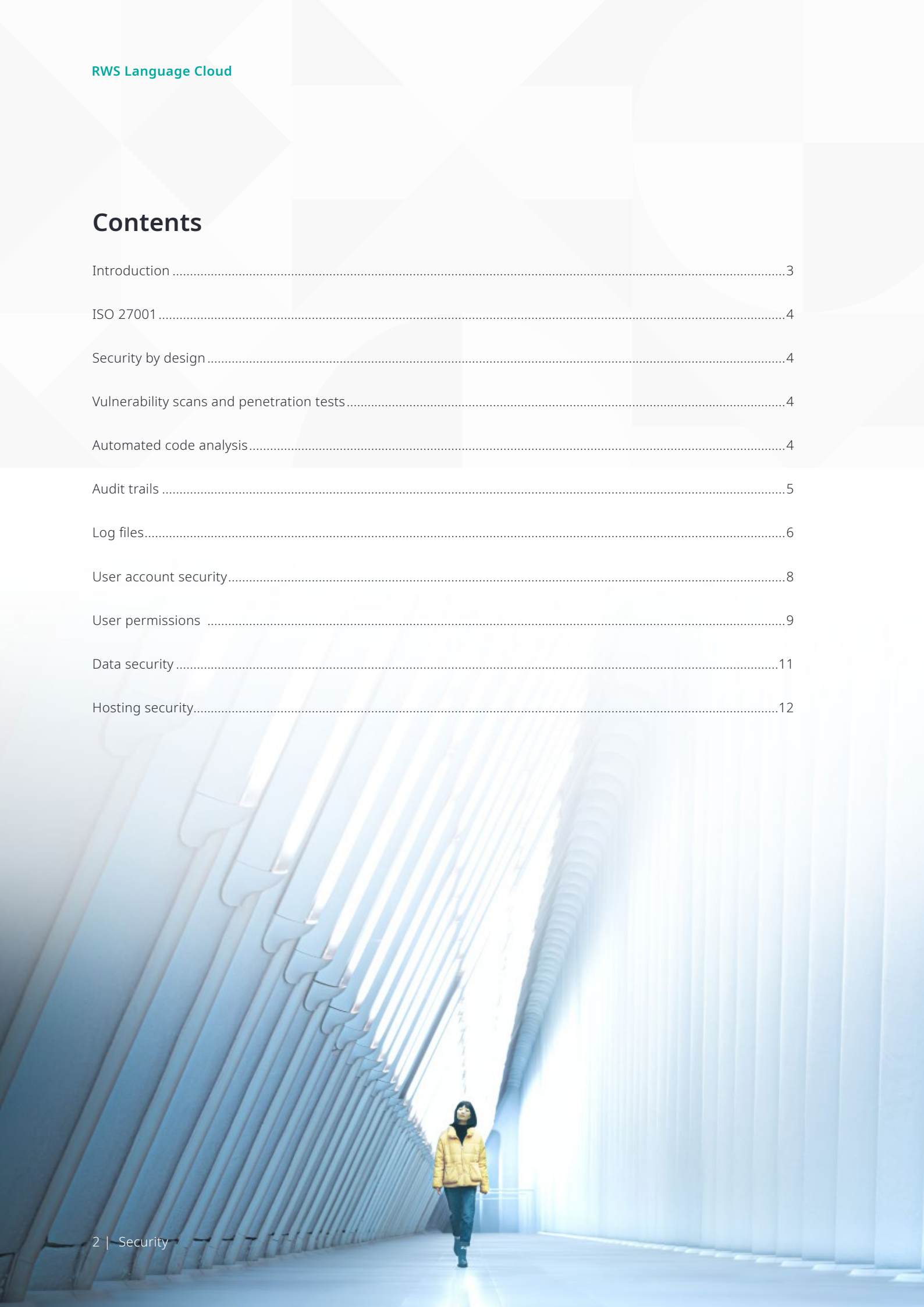


# RWS Language Cloud

Security

# Contents

Introduction .....	3
ISO 27001 .....	4
Security by design .....	4
Vulnerability scans and penetration tests .....	4
Automated code analysis .....	4
Audit trails .....	5
Log files .....	6
User account security .....	8
User permissions .....	9
Data security .....	11
Hosting security .....	12



## Introduction

The security of our customers' information is paramount to our business. RWS pledges to protect your business and data with state-of-the-art technology supported by our people, policies and procedures.

This paper details how we develop and host RWS® Language Cloud to ensure a secure environment in which you can process and manage content. These measures apply to all products that are hosted in Language Cloud, such as Trados® Enterprise, Trados® Accelerate, Trados® Team, and the cloud capabilities offered through Trados Studio®.



## ISO 27001

RWS Language Cloud's development organization is ISO 27001 certified, meaning the facilities, teams, policies and procedures used are regularly audited by independent, external assessors.



## Security by design

When creating new features and functionality in the product, we take a "security first" approach in accordance with our secure software development lifecycle. Extensive tests are carried out as part of the development process to ensure RWS Language Cloud continues to be a secure environment for the data that is processed; whether that data is content submitted for translation or data that relates to the users of the application.

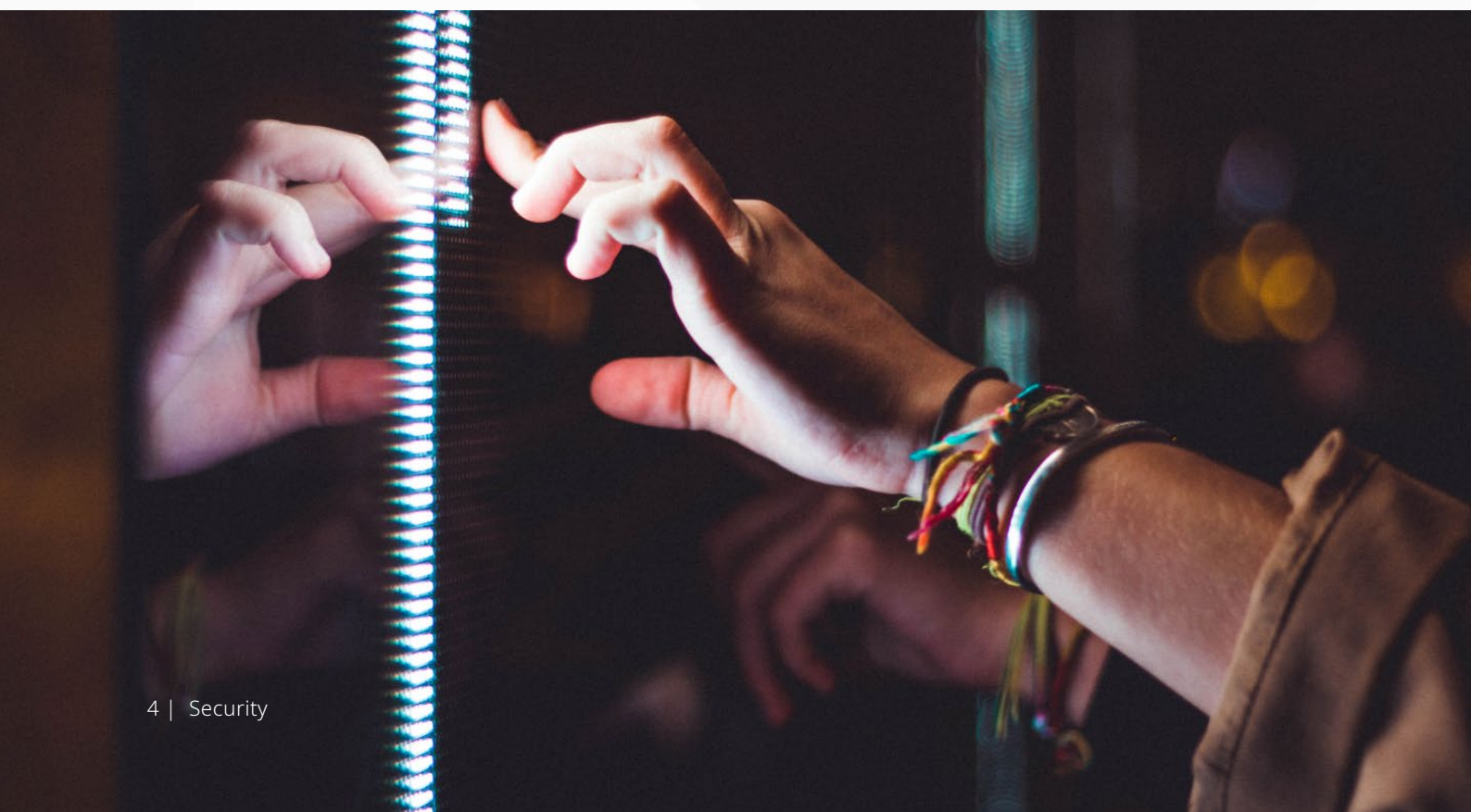
## Vulnerability scans and penetration tests

We regularly run rigorous vulnerability scans and penetration tests on the application. These always include testing against the OWASP Top Ten Web Application Security Risks. We engage annually with a third party to run external vulnerability and penetration tests. High and Critical level vulnerabilities are fixed as soon as possible. Medium and Low vulnerabilities are remediated based on risk or within a reasonable time.



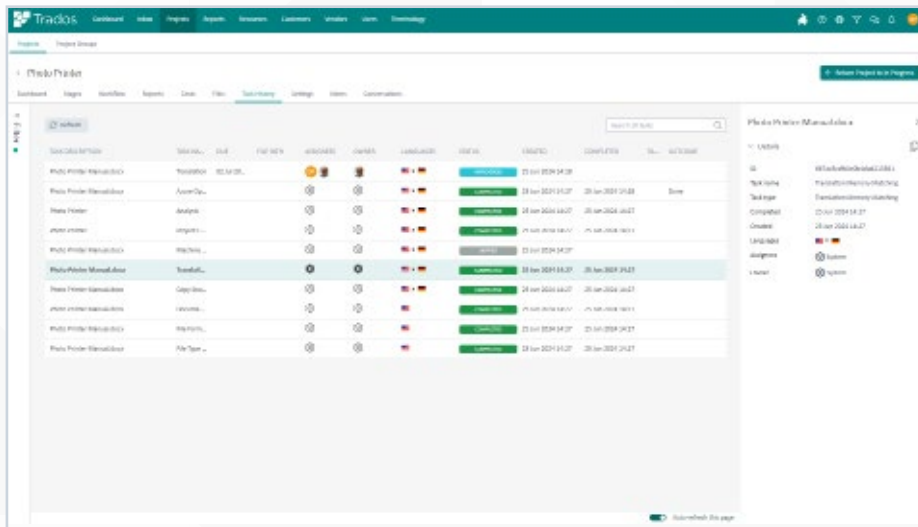
## Automated code analysis

In addition to penetration and vulnerability testing, all application source code is subjected to static application security testing (SAST) and dynamic application security testing (DAST). There are gates in place that fail the build if the quality threshold is not met. This failure is automatic and provides a sequence of auditable tests and retests if vulnerabilities are discovered.



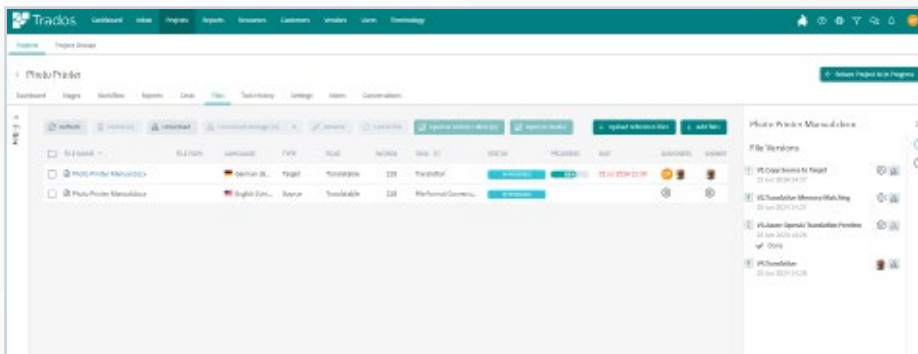
## Audit trails

RWS Language Cloud maintains a full audit trail of every file that is processed in the application. In the unlikely event of a security incident and potential data leak, a user with sufficient permissions (typically an administrator) can query the history of a file as it progressed through the workflow and determine which workflow tasks were executed on the file, and which users accessed the file.



Audit trail for files in a project.

RWS Language Cloud also keeps a history of all the versions of the file throughout its workflow lifecycle. The screenshot below shows the version history for a file as it went through various automated and human workflow tasks.



View version history for a file as it progresses through the workflow.

## Log files

RWS Language Cloud provides various log files that can be used in the event of a security incident.

### UI log files

Log files for users accessing the RWS Language Cloud application user interface (UI) are created and stored in standard NCSA combined log format. Example log entry:

```
10.228.144.254 - - [30/Aug/2024:03:08:14 +0000] "GET /lc/t/483384/dashboard HTTP/1.1"
200 14196 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.66 Safari/537.36" 761 14548 581839
```

These log files contain:

- **[host]** – The IP address or host/subdomain name of the client making the request
- **[rfc931]** – The identifier of the client making the request
- **[username]** – The username used by the client for authentication
- **[date:time timezone]** – The date and time stamp of the request
- **[request]** – The requested resource, the method, and the protocol version
- **[statuscode]** – The outcome of the request
- **[bytes]** – The number of bytes of data transferred
- **[referrer]** – The URL which linked the user to the site
- **[user\_agent]** – The web browser and platform used by the visitor
- **[cookies]** – One or more cookies passed by the browser



### Microservice log files

The RWS Language Cloud platform is a microservices architecture, which means there are many components (or services). Each service has a specific task and creates a log file. API requests are logged both at the platform inbound endpoint (API gateway) and within each internal component (service). Debugging information is also logged to aid in tracing specific behaviour. Examples:

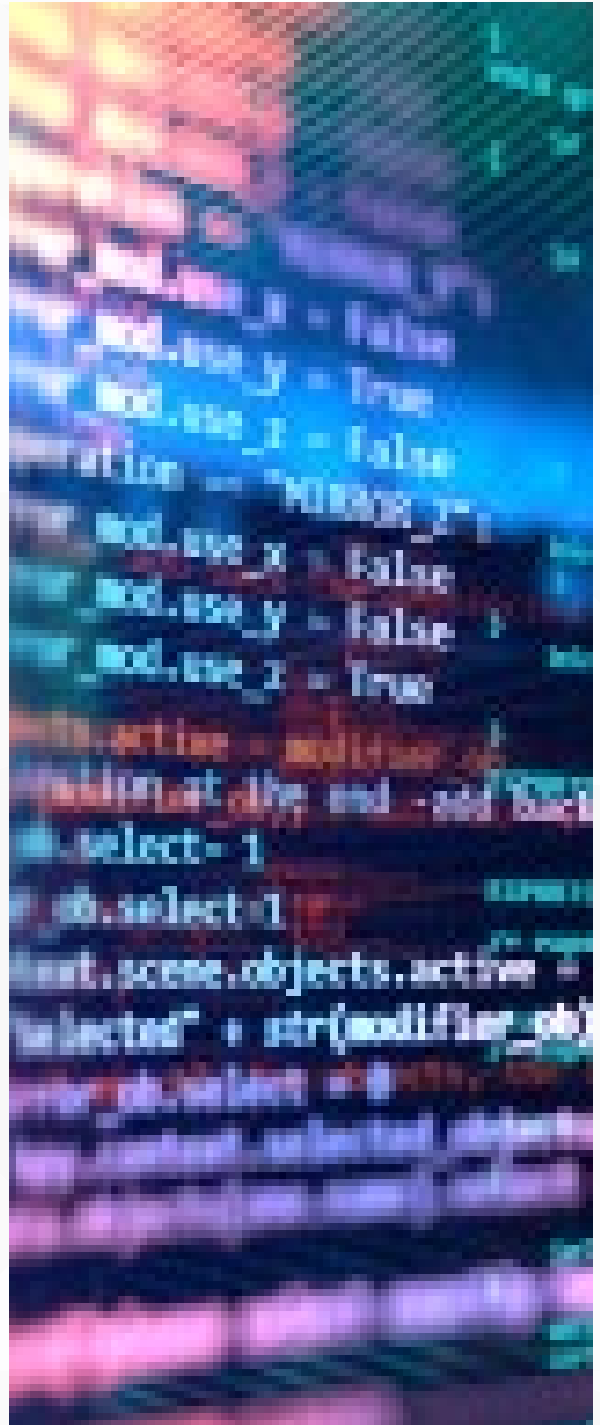
```
2024-09-01 07:45:31,880 INFO [http-nio-8765-exec-5179] [e76eafec-506f-4645-b6b2-d163ba173379] [lc.api.gateway] [guest] c.s.l.l.a.g.w.RequestLoggingConfiguration$1 [RequestLoggingConfiguration.java:35] Incoming request [GET /gw-account-web/accounts/5ee8b4e27b56b01e50b71a82/settings?tenant=461371, client=10.228.60.25, headers=[host:"de1-lc-apigw.sdlproducts.com", accept:"*/*", authorization:"masked", x-lc-caller-app:"LCUI/2.2.9", x-lc-appsid:"masked"]]
```

```
2024-09-01 07:45:32,004 INFO [http-nio-8080-exec-74] [e76eafec-506f-4645-b6b2-d163ba173379] [lc.account.service] [5ee8b4e27b56b01e50b71a82] c.s.l.g.a.s.a.AccountServiceImpl [AccountServiceImpl.java:1484] getAccountSettings >> 5ee8b4e27b56b01e50b71a82
```

```
2024-09-01 07:45:32,011 DEBUG [http-nio-8080-exec-74] [e76eafec-506f-4645-b6b2-d163ba173379] [lc.account.service] [5ee8b4e27b56b01e50b71a82] c.s.l.g.a.s.r.SubscriptionRepositoryImpl [SubscriptionRepositoryImpl.java:191] There is no subscription in cache for accountId=5ee8b4e27b56b01e50b71a82 sandbox=true
```

### Log monitoring and retention

By default, logs are kept for 90 days in a centralized logging server. Basic log monitoring is in place and internal API errors are monitored automatically, with an alert raised to an internal collaboration tool if the number of errors exceeds a pre-set threshold.





## User account security

RWS Language Cloud incorporates various features that facilitate user security.

### RWS ID

Every user of RWS Language Cloud must have an RWS ID to access it. RWS ID is a single-sign-on (SSO) solution based on a third-party identity platform provided by Auth0, a respected provider with first-class security credentials. For more information on Auth0 security, visit [auth0.com/security](https://auth0.com/security)

### Federation

RWS ID can be federated to your identity provider which provides the same levels of security as are present in your own environment. Options for federation include LDAP, ADFS, Azure Active Directory, OpenID Connect, SAML and others.

### Multi-factor authentication

If RWS ID is not federated to your identity provider, multi-factor authentication (MFA) can be implemented on a per-domain basis. MFA is an authentication method by which a user is granted access only after successfully presenting two or more pieces of evidence (factors) to an authentication mechanism:

- **Knowledge** (something the user knows, such as a password)
- **Possession** (something the user has, such as a mobile device)
- **Inheritance** (something the user is, such as a fingerprint)

### Session timeout

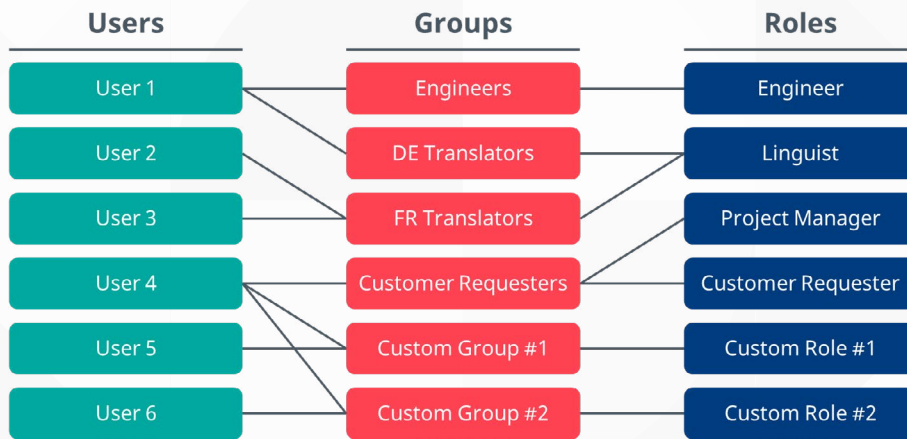
If a session is left inactive in RWS Language Cloud, it will automatically time out. The user will need to re-authenticate to continue working in the application.





## User permissions

In RWS Language Cloud, each user belongs to one or more user groups, and each group is assigned one or more roles. A role (set of permissions) determines which actions members of the group can execute at which level of the hierarchy. The role of a user who is a member of multiple groups is determined by creating a superset of all the roles of those groups.



Users and groups are managed by account administrators. If you're using a managed service, the account administrators will be RWS personnel who set up the users and groups, but do not subsequently have access to your data. Alternatively, you can administer your own users and groups without any involvement from RWS.

Jane Smith

**First name \***

**Last name \***

**Email \***

**Location \***

**Groups \***

PM Project Managers x
 A Administrators x
 E Engineers x
 ▼

T Terminologists x

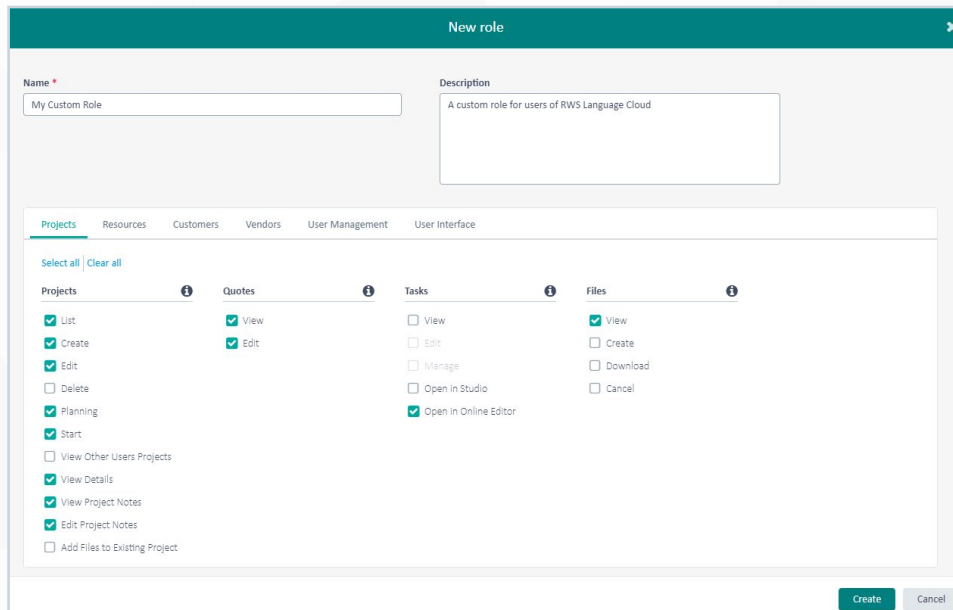
**Domains**

M Manufacturing x
 I IT x
 ▼

Add users and assign them to groups in the platform.

### Custom roles

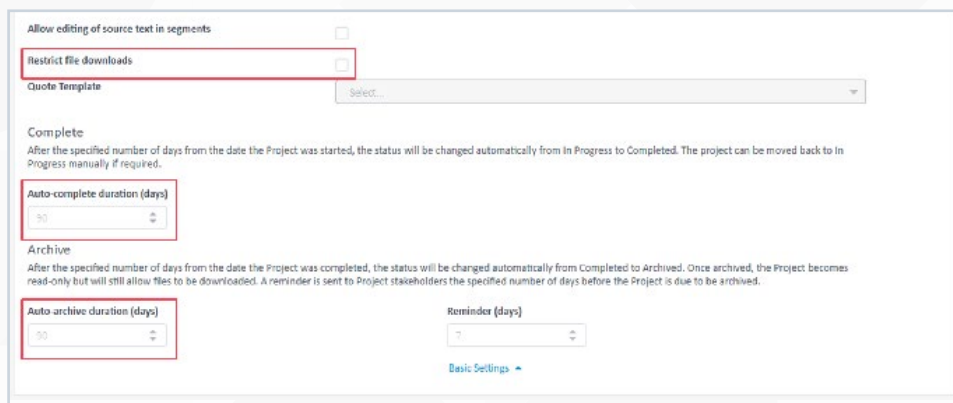
In addition to the default roles provided, RWS Language Cloud allows you to create custom roles that can be assigned to groups. A custom role can be granted a set of permissions, which allows flexibility when determining the actions that can be performed by the members of those groups.



Creating a new custom role.

### Project settings

Extra project settings that can also be configured. If you select the checkbox for Restrict file downloads, users will not be able to download files for offline translation. Instead, they will be required to complete their work in the online editor. Projects can also be automatically completed and archived after a specified number of days to prevent data from being accessed if those projects are unintentionally left active.



Edit project settings to restrict access to project data.

## Data security

RWS is committed to complying with all applicable data privacy and security laws in the countries in which it operates and hosts data.

### PII used to create an account

PII, or Personally Identifiable Information, refers to any information connected to an individual that can be used to uncover their identity. RWS ID stores minimal information about users (such as name and email address) and does not make this data available to other systems. The PII associated with a user can be edited, exported and deleted on request.

### PII in content submitted for translation

RWS Language Cloud does not currently have any provision for automatic anonymization or pseudonymization. If either is required, it is up to the customer to anonymize or pseudonymize the data before submitting it to RWS Language Cloud for translation.

### Encryption at rest

All data resident in the application is encrypted at rest. We also use secure protocols when transferring data. Data downloaded to a user's local system, however, is not guaranteed to be encrypted, but this risk can be mitigated by using the secure projects feature.

### Separation of data

Each customer's data is logically separated from every other customer's data, so it is not possible for customers to "see" each other's data. RWS Language Cloud uses metadata for tenant-level separation. Tenant isolation at runtime is enforced using dynamically generated identity and access management policies in line with best practices.

### Testing data

Development and testing environments are separate from the production environment so there is no data held in common. Unless we are given specific permission to do so, we will never use customer data in a testing or development environment.

### Data residency

RWS Language Cloud is hosted in AWS Frankfurt and AWS Montreal. Customers can choose the location where they want their data located. Once chosen, all customer data is held in the requested location. Backups for AWS Frankfurt are held in AWS Ireland. Backups for AWS Montreal are held in AWS Calgary.

### Security of data when using AI features

The AI features available in RWS Language Cloud are designed, developed, deployed, operated, and maintained with the same security measures as for the rest of the application features. RWS recognises that customers own their own data and must be in control of where it is used. Our AI features do not use customer data to help train or fine-tune Large Language Models (LLMs). When using AI-powered features, we rely on AI models that fall into one of two categories:

- **RWS-controlled**  
RWS-controlled AI models are hosted in our AWS infrastructure which means that customer data never leaves our core hosting environment.
- **Customer-controlled**  
Where customers are using an external AI model, data is transferred securely to and from this model. The security of the data within the model is the responsibility of the customer.



## Hosting security

### Hosting environment security

RWS Language Cloud is hosted as a SaaS application by RWS Cloud Operations, who are ISO 27001 certified for all our hosted products and have achieved 100% compliance with the controls and objectives of SOC 2 Type 2 attestation.

In addition, Cloud Operations have a collection of security tools and capabilities to ensure the security of our customers' data. These include:

- Event management monitoring tools to perform anomaly detection
- Perimeter firewalls and integrated network threat protection (NTP) with antivirus
- 24/7 operation to support real-time event management activities
- Industry-recommended tools for threat visibility
- A state-of-the-art vulnerability and penetration security testing scanner
- An IT Infrastructure Library (ITIL) compliant ticketing tool for incident management

### Hosting provider security

We have contracted with Amazon Web Services (AWS) to host our products. AWS maintains multiple certifications for security including ISO 27001, SSAE 16, SOC 1, SOC 2, and SOC 3. In addition to the security measures implemented by our hosting partners, we also have policies and procedures covering:



Access control



Data security



Physical protection



Availability and proactive monitoring



Logical protection



Risk assessment



Data backup

### Antivirus

All files uploaded to RWS Language Cloud are automatically scanned by antivirus software. Any files that are flagged as having malicious content are blocked for download and quarantined. RWS Language Cloud provides the capability to replace these files with non-infected versions.

**For more information about our approach to security, visit:**  
[rws.com/legal/security](https://rws.com/legal/security)

**To read our privacy policies, visit:**  
[rws.com/legal/privacy](https://rws.com/legal/privacy)

### About RWS

RWS Holdings plc is a unique, world-leading provider of technology-enabled language, content and intellectual property services. Through content transformation and multilingual data analysis, our combination of AI-enabled technology and human expertise helps our clients to grow by ensuring they are understood anywhere, in any language.

Our purpose is unlocking global understanding. By combining cultural understanding, client understanding and technical understanding, our services and technology assist our clients to acquire and retain customers, deliver engaging user experiences, maintain compliance and gain actionable insights into their data and content.

Over the past 20 years we've been evolving our own AI solutions as well as helping clients to explore, build and use multilingual AI applications. With 45+ AI-related patents and more than 100 peer-reviewed papers, we have the experience and expertise to support clients on their AI journey.

We work with over 80% of the world's top 100 brands, more than three-quarters of Fortune's 20 'Most Admired Companies' and almost all of the top pharmaceutical companies, investment banks, law firms and patent filers. Our client base spans Europe, Asia Pacific, Africa and North and South America. Our 65+ global locations across five continents service clients in the automotive, chemical, financial, legal, medical, pharmaceutical, technology and telecommunications sectors.

Founded in 1958, RWS is headquartered in the UK and publicly listed on AIM, the London Stock Exchange regulated market (RWS.L).

For further information, please visit: [www.rws.com](https://www.rws.com)

© 2024 All rights reserved. Information contained herein is deemed confidential and the proprietary information of RWS Group\*.

\*RWS Group shall mean RWS Holdings plc for and on behalf of its affiliates and subsidiaries.